



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/085,839	02/25/2002	Michael A. Kozuch	42P10794	1747
8791	7590	09/01/2006	EXAMINER	
BLAKELY SOKOLOFF TAYLOR & ZAFMAN				GEE, JASON KAI YIN
12400 WILSHIRE BOULEVARD				ART UNIT
SEVENTH FLOOR				PAPER NUMBER
LOS ANGELES, CA 90025-1030				2134

DATE MAILED: 09/01/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)
	10/085,839	KOZUCH ET AL.
	Examiner	Art Unit
	Jason K. Gee	2134

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) Responsive to communication(s) filed on 10 July 2006.
- 2a) This action is FINAL. 2b) This action is non-final.
- 3) Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) Claim(s) 1-47 is/are pending in the application.
 - 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) Claim(s) _____ is/are allowed.
- 6) Claim(s) 1-47 is/are rejected.
- 7) Claim(s) _____ is/are objected to.
- 8) Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) The specification is objected to by the Examiner.
- 10) The drawing(s) filed on 25 February 2002 is/are: a) accepted or b) objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
 - a) All b) Some * c) None of:
 1. Certified copies of the priority documents have been received.
 2. Certified copies of the priority documents have been received in Application No. _____.
 3. Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- 1) Notice of References Cited (PTO-892)
- 2) Notice of Draftsperson's Patent Drawing Review (PTO-948)
- 3) Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date _____.
- 4) Interview Summary (PTO-413)
Paper No(s)/Mail Date _____.
- 5) Notice of Informal Patent Application (PTO-152)
- 6) Other: _____.

DETAILED ACTION

1. This action is response to communication: amendment filed on 07/10/2006.
2. Claims 1-47 are currently pending in this application. Claims 1, 12, 21, 32, and 39 are independent claims. Claims 1, 12, and 21 have been amended.

Claim Objections

Claim 8 is objected to under 37 CFR 1.75(c), as being of improper dependent form for failing to further limit the subject matter of a previous claim. Applicant is required to cancel the claim(s), or amend the claim(s) to place the claim(s) in proper dependent form, or rewrite the claim(s) in independent form. Independent claim 1 has been amended to include all the limitations of claim 8, and claim 8 no longer further limits claim 1.

Claim Rejections - 35 USC § 112

3. The following is a quotation of the second paragraph of 35 U.S.C. 112:

The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.
4. Claim 10 is rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

As per claim 10, the recitation of trademarks such as Windows® should not be included in claims. Trademarks can change over time, and impact indefinite language to claims.

Response to Arguments

5. Applicant's arguments filed 07/10/2006 have been fully considered but they are not persuasive.
6. As per claim 10, the applicants have argued that there is no trademark recitation. However, claim 10 recites Windows NT, which is a registered trademark of Microsoft, with the trademark serial number of 74212523.
7. As per the independent claims, the applicants have argued that recording a hash digest of the content of the identified region is not taught. However, this is explicitly taught, as stated in the previous action, in col. 5 lines 50-65 of England '164. It is also cited explicitly in this section that a digest is stored in a register in the memory. Schneier's Applied Cryptography teaches signing documents with public keys. It also cites "only if she wished to prove her copyright would she have to make the document public" (page 39). This paragraph teaches that hashes may be signed and stored, and it is made available to the public (which are third parties) by proving a copyright.
8. The applicants have cited that they have amended independent claims 32 and 39 to overcome the previous art rejections, but no amendments have been made to the claims.

Claim Rejections - 35 USC § 103

9. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

10. Claims 1-9, 11-47 are rejected under 35 U.S.C. 103(a) as being anticipated by England et al. US Patent No. 6,938,164 (hereinafter '164), in view of Bruce Schneier's *Applied Cryptography* (Second Edition).

As per independent claim 1, '164 teaches a method of loading a trustable operating system. A region of memory is identified (col. 2 lines 16-21 and col. 4 line 54 to col. 5 line 12) by a processor. This computer may have multiple processors (col. 3 lines 9-13). Content is then loaded into this identified region (col. 5 lines 5-20). The processor then jumps to a known entry point in the content (col. 11 line 63 to col. 12 line 20). Also, '164 teaches registering an identity of the content of the identified region, the registering comprises: recording a hash digest of the content of the identified region ('164 col. 5 lines 49-65), and storing a hash digest in a register in the memory of the computer (col. 5 lines 49-65). However, signing a hash digest is not explicitly taught in '164. This is taught by Schneier though, in pages 38 and 39. Schneier teaches in pages 38-39 the signing of a hash digest which third parties can verify. Third parties

can verify this, as it is stated in Schneier that the documents may be copyrighted and can be proved by the public (which is making it accessible to a third party to verify).

At the time of the invention, it would have been obvious to one of ordinary skill in the art to include signing a hash digest in a system that registers an identity using a hash digest protocol. One of ordinary skill in the art would have been motivated to perform such an addition to save time. Schneier dictates on page 38 that "To save time, digital signature protocols are often implemented with on-way hash functions.... Instead of signing a document, Alice signs the hash of the document." Also, '164 indicates that additional information on hashing can be found in Schneier: "the reader is directed to a text written by Bruce Schneier and entitled "Applied Cryptography: Protocols, Algorithms, and Source Code in C," published by John Wiley & Sons with copyright 1994 (or second edition with copyright 1996)" (col. 5 lines 61-65), and therefore, it is obvious to combine the teachings of Schneier's Applied Cryptography.

As per claim 2, preventing interference with the identifying, loading, and registering by at least one of a remaining one of the plurality of processors are taught in col. 2 lines 11-25. '164 dictates "According to one aspect, a memory controller prevents CPUs and other I/O bus masters from accessing memory during a code (for example, OS, microkernel, or other trusted core) initialization process." Since this method prevents CPUs to access memory, it will restrict it from identifying, loading, and registering as memory cannot be accessed. Identifying, loading, and registering is taught in col. 9 line 57 to col. 10 line 11.

As per claim 3, preventing interference comprises halting at least one of the remaining ones of the plurality of processors until the identifying, loading, and registering is complete (col. 2 lines 10-25). The other processors are halted as they are being reset. '164 dictates "Once an initialization process has been executed by that CPU, the code is operational and any other CPUs are allowed to access memory (after being reset), as are any other bus masters (subject to any controls imposed by the initiated code)." Identifying, loading, and registering is taught in col. 9 line 57 to col. 10 line 11.

As per claim 4, causing at least one of the remaining ones of the plurality of processors to jump to the known entry point in the content is taught in col. 2 lines 10-25, as it states that "other CPUs are allowed to access memory" after the initialization process is complete.

As per claim 5, identifying comprises receiving a region parameter, the region parameter specifying a location of the region. This is taught in col. 9 lines 59-62, where it indicates that the start parameter "refers to the location in memory 110 where trusted core 146 begins (e.g., the memory address of the first instruction of platform trusted code portion 148)."

As per claim 6, the location comprises a range of addresses in the memory of the computer within which the region is located. Addresses are taught already in the rejection for claim 5 above, and can also be found in col. 11 line 63 to col. 12 line 20 and also col. 14 lines 55-65. Also, col. 10 line 55 to col. 11 line 15 indicate a range of addresses that can be accepted.

As per claim 7, the location comprises a start address and a length of the memory of the computer within which the region is located. This is taught in col. 9 lines 57-67: "the Trusted Core Initialization command includes three parameters: start, length of code, and length of memory ... the start parameter refers to the location in memory where trusted core begins (e.g., the memory address of the first instruction...").

Claim 8 is rejected using the same basis of arguments used to reject claim 8 above.

As per claim 9, '164 teaches that the content is a component of an operating system to operate the computer. Col. 5 lines 13-20 indicate this: "Various components 144 of an operating system are thus laded into memory 110"

As per claim 11, '164 teaches that loading and registering are uninterruptible. Col. 14 lines 45-54 indicate that interrupts are disallowed during the initialization process. It is already rejected in the above claims that the initialization process comprises loading and registering.

As per independent claim 12, '164 teaches halting all but one of plurality of central processing units in a computer (col. 2 lines 10-25). A region of memory is identified (col. 2 lines 16-21 and col. 4 line 54 to col. 5 line 12) by a processor. This computer may have multiple processors (col. 3 lines 9-13). Content is then loaded into this identified region (col. 5 lines 5-20). The processor then jumps to a known entry point in the content (col. 11 line 63 to col. 12 line 20). Blocking access to the identified region by all resources except the non-halted CPU is taught in col. 10 line 55 to col. 11 line 15. Recording a cryptographic hash of the content of the identified region is taught

in col. 5 line 49 to col. 6 line 5. Causing the non-halted CPU to begin executing at a known entry point in the identified region is taught in col. 11 line 63 to col. 12 line 20. Signing the cryptographic hash, storing the hash in a register in the memory that is accessible to a third party to verify whether the content can be trusted is rejected using the same basis of arguments used to reject claim 1.

As per claim 13, '164 teaches that the data that causes the machine to halt all but one of a plurality of CPUs comprises data causing the all but one of a plurality of CPUs to enter a halted state: "CPUs can be prevented from issuing read and write requests on processor bus 112, or by issuing a halt (e.g., HLT) command to the CPUs which halts the operation of each CPU until it resets" (col. 10 lines (62-67).

As per claim 14, '164 teaches that the data further causes the halted CPUs to exit the halted state after the non-halted CPU has begun executing at the known entry point in the identified region. This is taught in col. 2 lines 10-25, where the CPUs are reset and allowed to access memory through the initiated code.

As per claim 15, '164 teaches in col. 2 lines 10-25 that the data further causes the previously halted CPUs to begin executing at the known entry point in the identified region upon exiting the halted state: "Once an initialization process has been executed by that CPU, the code is operational and any other CPUs are allowed to access memory (after being reset), as are any other bus masters."

As per claim 16, '164 teaches recording the computed cryptographic hash in a hash digest area in col. 5 line 49 to col. 6 line 5. It indicates that the digest can be found in a register, which is a hash digest area. Computing the cryptographic has of the

identified region is taught in col. 5 lines 49-65. A required platform information is recorded in the hash digest area, as '164 indicates that the digest contains a value that can be considered to uniquely represent the trusted core in use. Erasing a hash digest area (which is a register) is taught in col. 12 lines 31-39. This section teaches that a CPU clears the states of the CPU, which is located in the registers.

As per claim 17, '164 teaches in col. 5 line 49 to col. 6 line 5 that a hash digest area is a register in the memory of the computer.

Claim 18 is being rejected using the same basis of arguments used to reject claim 5.

Claim 19 is being rejected using the same basis of arguments used to reject claim 6.

Claim 20 is being rejected using the same basis of arguments used to reject claim 7.

As per independent claim 21, '164 teaches halting all but one of plurality of central processing units in a computer (col. 2 lines 10-25). Blocking access to the identified region by all resources except the non-halted CPU is taught in col. 10 line 55 to col. 11 line 15. Recording a cryptographic hash of the content of the identified region is taught in col. 5 line 49 to col. 6 line 5. Placing the non-halted CPU into a known privileged state is taught in col. 6 lines 38-63. Signing the cryptographic hash, storing the hash in a register in the memory that is accessible to a third party to verify whether the content can be trusted is rejected using the same basis of arguments used to reject claim 1.

As per claim 22, jumping to a known entry point in the region is taught in (col. 11 line 63 to col. 12 line 20).

As per claim 23, '164 teaches that halting comprises causing the all but one of a plurality of CPUs to enter a special halted state (col. 10 line 55 to col. 11 line 15). This halted state is special as only the CPUs that need to be halted receive this 'HLT' command.

As per claim 24, '164 teaches exiting the special halted state after the non-halted CPU has begun executing at the known entry point in the identified region. This is taught in col. 2 lines 10-25, where the CPUs are reset and allowed to access memory through the initiated code.

As per claim 25, '164 teaches in col. 2 lines 10-25 that the data further causes the previously halted CPUs to begin executing at the known entry point in the identified region upon exiting the special halted state: "Once an initialization process has been executed by that CPU, the code is operational and any other CPUs are allowed to access memory (after being reset), as are any other bus masters."

Claim 26 is rejected using the same basis of arguments used to reject claim 16.

Claim 27 is rejected using the same basis of arguments used to reject claim 17.

As per claim 28, col. 5 lines 49-65 teach computing a cryptographic hash of the region's contents. Something that can perform a digest hashing function can be considered a digest signing engine. This is coupled to the memory of a computer, as the hash digest is stored. This is also described in col. 11 lines 45-62.

Claim 29 is being rejected using the same basis of arguments used to reject claim 5. This location is secured, as taught in col. 9 lines 62-67.

Claim 30 is being rejected using the same basis of arguments used to reject claim 6. Col. 11 line 63 to col. 12 line 20 indicate that the addresses are of the trusted core, which is secure.

Claim 31 is being rejected using the same basis of arguments used to reject claim 7. This region is secured, as this is part of the initialization sequence by the trusted core.

As per independent claim 32, '164 teaches an apparatus to load a trustable operating system. '164 is directed toward an apparatus that can allow code to be securely initiated in a computer, which can be considered a start secure operation. Col. 2 lines 10-25 teaches that a processor initiates the process. This startup operation has a memory region parameter, as these lines discuss a memory controller and a restriction of access to a memory by other processors when initialization has started. Blocking access to a region of memory is taught in these lines as well, as it dictates that a memory controller prevents other CPUs to access the memory. Content is then placed into this memory, as described in col. 5 lines 13-20. A cryptographic hash of the content of the specified region is recorded in the hash digest, as described in col. 5 lines 49-65. This can also be erased, as taught in col. 12 lines 31-39. This section teaches that a CPU clears the states of the CPU, which is located in the registers. Unblocking access is taught in col. 2 lines 10-25, where access is allowed after the initialization process and the other CPUs are reset. Jumping to a known entry point in the content of

the specified region is taught in col. 11 line 63 to col. 12 line 20. It is noted that the claim states 'is capable.' A system 'capable' to perform an action indicates that the method is not prohibiting the action from happening. Thus, anything that doesn't stop these things from occurring appears to meet the claim limitations. This holds true for claims 32-37.

As per claim 33, '164 teaches in col. 10 line 55 to col. 11 line 15 that a second processor is prevented from interfering with the first processor's initialization process (SS). The other CPUs can execute this process, as indicated in these lines, and this process can be named a join secure operation (JSO).

As per claim 34, '164 teaches in col. 2 lines 10-25 that when the first processor undergoes the initialization process (SSO), the other CPUs undergo a process in which they cannot interfere with the initialization process (JSO).

As per claim 35, the second processor enters a halted state until the first processor's execution of the initialization process (SSO) is complete. This is taught in col. 10, lines 55-67, where CPUs are halted until they are reset. It is taught in col. 2 lines 10-25 that the CPUs are reset after the first processor has been executed.

As per claim 36, '164 teaches in col. 2 lines 10-25 that a second processor exits the halted state after the first processor's execution of the SSO is complete. This section also indicates that the second processor is then allowed to access the memory in which it was restricted from earlier.

Claim 37 is being rejected using the same basis of arguments used to reject claim 28. Col. 5 lines 49-65 teach computing a cryptographic hash, and a digest signing engine would be necessary for a computing element to compute this hash. Details are also found in col. 11 lines 45-62.

As per claim 38, the cryptographic hash is stored in the digest 138 or in a register, as indicated in col. 5 line 49 to col. 6 line 5. This is outside the specified region memory 110 indicated in col. 5 lines 21-25.

As per independent claim 39, '164 teaches a method of loading a trustable operating system. Selecting an area in a memory accessible to a processor is taught in col. 2 lines 10 –25, where it indicates that it allows a CPU to access a memory at a particular location. Loading a data into the selected area is taught in col. 5 lines 13-30. Directing the processor to commence processing at an entry point in the selected area is taught in col. 11 line 63 to col. 12 line 20. And preventing interruption of selecting, loading, and directing is taught in col. 2 lines 11-25. '164 dictates "According to one aspect, a memory controller prevents CPUs and other I/O bus masters from accessing memory during a code (for example, OS, microkernel, or other trusted core) initialization process." Since this method prevents CPUs to access memory until the first processor finishes initializing and the other CPUs are reset, it will prevent the selecting, loading, and directing until they are completed. The selecting, loading, and directing taught above are part of the initialization process.

As per claim 40, halting any other processors having access to the memory until the selecting, loading, and directing is complete is taught in col. 10 line 55 to col. 11 line

15. These processors are halted until they are reset, and they are reset after the initialization process is complete, as indicated in col. 2 lines 10-25.

As per claim 41, causing the other processors to commence processing at an entry point in the selected area is taught in col. 2 lines 10-25, where the other CPUs are allowed to access the memory. It is also taught in col. 10 line 55 to col. 11 line 15 that the other CPUs are allowed to access the memory within an address range of the trusted core memory.

As per claim 42, receiving a parameter specifying a location of the area to be selected is taught in col. 9 lines 59-62, where it indicates that the start parameter “refers to the location in memory 110 where trusted core 146 begins (e.g., the memory address of the first instruction of platform trusted code portion 148).”

As per claim 43, the location comprises a range of addresses in the memory of the computer within which the region is located. Addresses are taught already in the rejection for claim 5 above, and can also be found in col. 11 line 63 to col. 12 line 20 and also col. 14 lines 55-65. Also, col. 10 line 55 to col. 11 line 15 indicate a range of addresses that can be accepted.

As per claim 44, the location comprises a start address and a length of the memory of the computer within which the region is located. This is taught in col. 9 lines 57-67: “the Trusted Core Initialization command includes three parameters: start, length of code, and length of memory ... the start parameter refers to the location in memory where trusted core begins (e.g., the memory address of the first instruction...”).

Claim 45 is rejected using the same basis of arguments used to reject claim 8 above. Registering an identity of the data loaded in the selected area is taught in the rejection for claim 2 above and also in col. 5 lines 49 to col. 6 line 5.

Claim 46 is rejected using the same basis of arguments used to reject claim 9. The memory resides in this device, as it is an internal memory, as indicated in col. 5 lines 5-12.

As per claim 47, '164 indicates in col. 5 lines 13-20 that the operating systems can be Windows® operating systems. It is inherent that Windows® has a graphical user interface.

11. Claim 10 is rejected under 35 U.S.C. 103(a) as being unpatentable over '164 and Schneier as applied above, and further in view of ATPM – Review: Virtual PC 4.0 (April 2001), by Gregory Tetrault.

As per claim 10, col. 5 lines 13-20 indicate various operating systems. These lines describe the Windows® operating systems. A privileged software nucleus is taught in col. 6 lines 38-63, in which different privilege levels are taught. However a virtual machine monitor is not taught in '164. However, this is taught in ATPM's review of Virtual PC, reviewed by Gregory Tetrault. ATPM indicates that Windows® supported virtual machine.

At the time of the invention, it would have been obvious to one of ordinary skill in the art to include the use of virtual machines when using Windows® operating systems.

One would have been motivated to perform such an addition, because a virtual machine is an option provided by operating systems such as Windows®, and is useful for networking. Col. 3 lines 4-14 of '164 indicates that the invention can apply to network PCs as well, and a virtual machine is an example of a network PC.

Conclusion

12. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

13. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Jason K. Gee whose telephone number is (571) 272-6431. The examiner can normally be reached on M-F, 7:00 am to 4:30 pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Jacques Louis-Jacques can be reached on (571) 272-6962. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Jason Gee
Patent Examiner
Technology Center 2134
08/30/06

Jacques Louis-Jacques
JACQUES LOUIS-JACQUES
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100